



EFCOG Safeguards and Security Working Group

# Program Review 10 CFR Part 824

Program Implementation Matrix

B.W. Avery PNNL  
1/7/2009

PROGRAM REVIEW 10 CFR PART 824 PROGRAM IMPLEMENTATION

#	Question/ Criteria/ Action	Team Action	Documents Reviewed/ Individuals Interviewed	Response/ Comments	Results (S, W/PI, ME, N/A)

This matrix is to help DOE contractors validate the performance of the necessary protection elements for the protection of classified information. It helps provide assurances to DOE that proper management and supervisory systems are in place to assure that all activities are carried out in compliance with classified information security requirements.

HS – 43 Integrated Program Review (IPR) Scope:

- Security Incident Program
- Self Assessment Process – Corrective Action Plans (CAPs)
- Security Survey/Inspection Results – CAPs
- Security Incident Trending Results – 24 Months
- Integration with the Enforcement Coordinator
- CMPC Program
- Classified Cyber Security Program

PROGRAM REVIEW 10 CFR PART 824 PROGRAM IMPLEMENTATION

#	Question/ Criteria/ Action	Team Action	Documents Reviewed/ Individuals Interviewed	Response/ Comments	Results (S, W/PI, ME, N/A)
---	----------------------------	-------------	---	--------------------	----------------------------

<b>G</b> <i>General Program Descriptions</i>					
1	Is there an overall description of the classified information security program?	Review program documentation to determine if there is a clear description of the classified information protection program (and 10 CFR 824 elements).	<i>Suggested: Program Description documents</i>		
2	Are management and assurance systems in-place to ensure that all activities are in compliance with the DOE classified information security requirements?	Review program documentation and interview key program staff to determine if there is a clear information protection program with appropriate levels of instruction/procedures and management oversight.	<i>Suggested: Information Protection Procedures; Management System/ organizational descriptions, SSSP or SSP, internal assessment results and external audit results</i>		
<b>R</b> <i>Roles and Responsibilities</i>					
3	What are the specific roles and responsibilities associated with the program? Are key senior managers designated with responsibility for major security programs? Do they have the authority to set requirements and provide oversight (Classified Information	Review organizational charts and interview sr. management to determine if clear roles, responsibilities and authorities are delineated for this program.	<i>Suggested: Org Charts and Management System/ organizational descriptions, SOP's</i>		

PROGRAM REVIEW 10 CFR PART 824 PROGRAM IMPLEMENTATION

#	Question/ Criteria/ Action	Team Action	Documents Reviewed/ Individuals Interviewed	Response/ Comments	Results (S, W/PI, ME, N/A)
	Protection/Control, Cyber)?				
4	How does Safeguards and Security (S&S) interface with senior management?	Review program documentation and interview S&S and senior management to determine degree of interface.	<i>Suggested: Program descriptions; meeting minutes. Trending results, internal assessment results and external audit results</i>		
5	How is senior management's support of S&S demonstrated?	Interview S&S and senior management to identify how management support is achieved.	<i>Budget and performance goals</i>		
6	Is an individual formally designated with the responsibility to review security non-compliances and report as appropriate to DOE?	Review program documentation and interview key staff/ management.	<i>Suggested: Organizational charts; Program descriptions; and/ or Position descriptions, SOPs</i>		
<b>PM</b>	<b>General Program Management</b> (Note: Details supporting many questions in this section are included in the sections that follow)				
7	Is communications related to the information protection program demonstrated internal to S&S as well as the line organizations?	Review program documentation and interview key S&S staff to determine if communications seem adequate.	<i>Suggested: Communication products; Procedures; Training, internal assessment results and external audit results</i>		
8	Are results, trends and issues being routinely reported to senior management? Are results of reviews being used to correct issues and prevent recurrence?	Review program documentation and interview key S&S staff to determine if reporting exists and if corrective action plans were developed.	<i>Suggested: Trend reports; internal assessment reports; Incident reports; Corrective Action plans.</i>		

PROGRAM REVIEW 10 CFR PART 824 PROGRAM IMPLEMENTATION

#	Question/ Criteria/ Action	Team Action	Documents Reviewed/ Individuals Interviewed	Response/ Comments	Results (S, W/PI, ME, N/A)
9	Are the requirements (DOE Orders, Manuals, directives, CFRs, etc.) applicable to the information protection and enforcement program identified and implemented? Reference: PR 24	Review program documentation and interview key S&S staff to determine if a process exists that identifies applicable requirements and their implementation.	<i>Suggested: Decision documents; Contract modifications; Procedures</i>		
10	Are S&S and the information protection organization integrated with the rest of the organization? Integration with the Enforcement Coordinator?	Review organization charts and interview key S&S management.	<i>Suggested: Organizational charts; Management system/program descriptions, SOPs</i>		
11	Is there a process to ensure rule requirements are understood and that requirements are effectively implemented down to the facility level, process and activity? Reference: PR 23	Review program documentation and interview key S&S and line staff/ management. Review training course materials. Review assessment expectations and processes.	<i>SOPs, Training, internal assessment results and external audit results</i>		
12	Is there a security problem resolution process in place that contains the following elements: ○ Manages issue prioritization ○ Assigns responsibility	Review program documentation and interview key S&S and line staff/ management.	<i>SOPs, Corrective Action process, Trending Results, and ISC Reports</i>		

PROGRAM REVIEW 10 CFR PART 824 PROGRAM IMPLEMENTATION

#	Question/ Criteria/ Action	Team Action	Documents Reviewed/ Individuals Interviewed	Response/ Comments	Results (S, W/PI, ME, N/A)
	<ul style="list-style-type: none"> <li>○ Evaluates and determines causes</li> <li>○ Identifies adverse trends and dominant security issues</li> <li>○ Determines extent of condition</li> <li>○ Develops corrective actions</li> <li>○ Tracks completion of corrective actions</li> <li>○ Independent validation to determine effectiveness of actions taken</li> </ul> Reference: I 32,33, 34, 36				
13	Do the methods for self identifying problems include the following: <ul style="list-style-type: none"> <li>○ Self assessments</li> <li>○ Internal review processes</li> <li>○ Worker identified</li> <li>○ External audits</li> <li>○ Trending and evaluation of operational data and issues management systems</li> <li>○ Employee concerns</li> </ul>	Review program documentation and interview key S&S and line staff/ management.	<i>SOPs, Corrective Action process, Trending Results, and SSIMS</i>		

PROGRAM REVIEW 10 CFR PART 824 PROGRAM IMPLEMENTATION

#	Question/ Criteria/ Action	Team Action	Documents Reviewed/ Individuals Interviewed	Response/ Comments	Results (S, W/PI, ME, N/A)
	<p>programs</p> <ul style="list-style-type: none"> <li>○ Events and Incidents</li> </ul> <p>Are issues identified through these methods put into appropriate problem resolution processes? Reference: I 27</p>				
14	<p>Are there metrics in place for the associated program areas? How are they monitored and reported? Is security incident reporting encouraged and/or incentivized? Reference: I 28</p>	<p>Review program documentation and interview key S&amp;S staff to determine if metrics are established, monitored and reported. Determine if they are reported with internal and DOE management.</p>	<p><i>SOPs, Trending Results, and SSIMS</i></p>		
15	<p>Are ISC's categorized correctly?</p>	<p>Review ISC program documentation</p>	<p><i>ISC Reports, SOP's, Trending Results, and SSIMS</i></p>		
16	<p>Is the S&amp;S staffing level appropriate?</p>	<p>Interview key S&amp;S staff and management to determine if staffing is appropriate.</p>	<p><i>ISC Reports – timely reporting and report completion</i></p>		
<b>T</b>	<b><i>Training and Awareness</i></b>				
17	<p>Do information protection programs have appropriate training and/or awareness courses for the line organizations? Are they</p>	<p>Identify training requirements, courses and tools that support each sub-area. Determine if appropriate reviews are</p>	<p><i>Suggested: Applicable training courses; Procedures detailing training requirements, SOPs</i></p>		

PROGRAM REVIEW 10 CFR PART 824 PROGRAM IMPLEMENTATION

#	Question/ Criteria/ Action	Team Action	Documents Reviewed/ Individuals Interviewed	Response/ Comments	Results (S, W/PI, ME, N/A)
	maintained current and monitored for effectiveness? Is 10 CFR 824 included	being conducted.			
18	Are there appropriate qualification requirements for S&S staff associated with the classified information security program elements?	Review S&S program documentation, training documentation and interview key S&S staff/ management to determine if S&S qualifications are documented and maintained.	<i>Suggested: Training documentation – expectations/ responsibilities, training records</i>		
19	Who performs causal analysis? What qualifications must they possess?	Review program documentation, training documentation and interview key S&S staff/ management to determine if qualifications have been established and documented. Review training records to determine if qualifications have been met.	<i>Suggested: Training documentation – expectations/ responsibilities, training records</i>		
20	Who performs non-compliance investigations or inquiries? What qualifications must they possess?	Review program documentation, training documentation and interview key S&S staff/ management to determine if qualifications have been established and documented. Review	<i>Suggested: Training documentation – expectations/ responsibilities, training records</i>		

PROGRAM REVIEW 10 CFR PART 824 PROGRAM IMPLEMENTATION

#	Question/ Criteria/ Action	Team Action	Documents Reviewed/ Individuals Interviewed	Response/ Comments	Results (S, W/PI, ME, N/A)
		training records to determine if qualifications have been met.			
21	Who performs assessments? What qualifications must they possess?	Review program documentation, training documentation and interview key S&S staff/ management to determine if qualifications have been established and documented. Review training records to determine if qualifications have been met.	<i>Suggested: Training documentation – expectations/ responsibilities, training records</i>		
22	Are individuals performing key S&S roles associated with the classified information security program routinely evaluated to determine if qualifications and or performance is meeting expectations?	Review S&S program documentation, other related documentation and interview key S&S staff/ management to determine if a process exists and is being followed.	<i>Suggested: Annual performance reviews</i>		
<b>PR</b>	<b><i>Procedures, General</i></b>				
23	Do adequate procedures exist to delineate requirements associated with classified information protection for line organization staff and management? Are they	Review internal documentation and interview appropriate S&S staff to identify the specific internal procedures that support each sub-area.	<i>Suggested: Information Protection Procedures</i>		

PROGRAM REVIEW 10 CFR PART 824 PROGRAM IMPLEMENTATION

#	Question/ Criteria/ Action	Team Action	Documents Reviewed/ Individuals Interviewed	Response/ Comments	Results (S, W/PI, ME, N/A)
	formally approved? Reference: PM 11				
24	Do adequate procedures exist to delineate requirements associated with classified information protection for S&S staff? Are they compliant with DOE requirements? Reference: PM 9	Review internal documentation and interview appropriate S&S staff to identify the specific internal procedures that support each sub-area.	<i>Suggested: Information Protection Procedures</i>		
25	Are procedures maintained in a current and up-to-date manner, with DOE Security policies?	Review documentation and interview appropriate S&S staff to determine if there is evidence of routine reviews.	<i>Suggested: Information Protection Procedures</i>		
<b>S</b>	<b><i>Subcontractors</i></b>				
26	Are processes in place to flow down requirements to subcontractors related to classified information protection?	Review procedures and interview appropriate S&S staff to determine if flow down of related requirements are being made. Review subcontractor information to validate requirements are appropriately flowed down.	<i>Suggested: Subcontracting Procedures, systems and contract language</i>	Do you have cleared subcontracts/ors? What is the level of security oversight/ interface with them? Are appropriate clauses included in the subcontracts (1- Security clause, 2-opt – Class/Declass clause)? How do you specify what orders apply (flow down/ documentation)? How are reporting requirements managed (i.e., incidents)? Self assessments – how are they managed for cleared subs? Non-possess – incidents and mgmt of classified at other locations – how managed?	
<b>I</b>	<b><i>Non-compliance Identification, Analysis, Reporting, Tracking and Closure</i></b>				

PROGRAM REVIEW 10 CFR PART 824 PROGRAM IMPLEMENTATION

#	Question/ Criteria/ Action	Team Action	Documents Reviewed/ Individuals Interviewed	Response/ Comments	Results (S, W/PI, ME, N/A)
27	How are non-compliances identified? Reference: PM 13	Review documentation and interview S&S staff to determine if a documented process exists. Validate that it includes incidents/ events as well as maintenance/ surveillance and employee concerns activities.	<i>Suggested: Information Protection (Incident/ Event/ Maintenance) Procedures, internal assessment results and external audit results</i>		
28	Is there a grading system applied to identified non-compliances (minor versus major)? Do they also include inadvertent versus willful? Is responsibility assigned? Are security incidents appropriately categorized per DOE requirements (e.g., IMI)? Reference: PM 14	Review documentation and interview S&S staff to determine if a documented grading system exists. Determine if major non-compliances have been identified.	<i>Suggested: Information Protection (Incident/ Event/ Maintenance) Procedures; Non-compliance reports and documentation, SSIMS</i>		
29	Have there been any assessments to evaluate if management of reported non-compliances follows the guidance?	Review documentation for self assessments of S&S processes.	<i>Suggested: Internal assessment results</i>		
30	Is the Enforcement Coordinator notified of security incidents, assessment/survey/inspection findings, and the sites trending results?	Review documentation for S&S processes and interview key S&S staff and Enforcement Coordinator	<i>Suggested: Procedures, SOPs, applicable trending reports, SSIMS</i>		

PROGRAM REVIEW 10 CFR PART 824 PROGRAM IMPLEMENTATION

#	Question/ Criteria/ Action	Team Action	Documents Reviewed/ Individuals Interviewed	Response/ Comments	Results (S, W/PI, ME, N/A)
31	How are significant issues, involving classified information, being reported to DOE?	Review documentation for of S&S processes and interview key S&S staff to determine if a standardized reporting system exists.	<i>Suggested: Procedures; Security incident notifications, SSIMS</i>		
32	Is the extent of condition determined for non-compliances? Does analysis of the event reflect an appropriate level of depth and breadth? Reference: PM 12, I 33, 34, 36	Review documentation for S&S processes and interview key S&S staff to determine if extent of conditions are being determined or considered.	<i>Suggested: Procedures; Non-compliance reports, internal assessment results, trend reports</i>		
33	Is causal analysis applied to identified non-compliances? Does the causal analysis (and investigations) include precursor/historical reviews? Reference: PM 12, I 32, 34, 36	Review documentation for of S&S processes and interview key S&S staff to determine if causal analysis are being determined or considered.	<i>Suggested: Procedures; Non-compliance reports, internal assessment results and external audit results, trend reports</i>		
34	Are corrective actions developed for identified non-compliances?	Review documentation for of S&S processes and interview key S&S staff to determine if corrective	<i>Suggested: Procedures; Non-compliance reports, corrective action processes, SSIMS, local discrepancy</i>		

PROGRAM REVIEW 10 CFR PART 824 PROGRAM IMPLEMENTATION

#	Question/ Criteria/ Action	Team Action	Documents Reviewed/ Individuals Interviewed	Response/ Comments	Results (S, W/PI, ME, N/A)
	Reference: PM 12, I 32, 33, 36	actions are being developed. Review selected corrective action documentation.	<i>management system</i>		
35	Are the corrective actions derived from causal analysis processes? Do they address the cause? Is there a direct relationship between causal analysis and the corrective action plans?	Review documentation for of S&S processes and interview key S&S staff to determine if corrective actions are being developed from causal analysis results. Review selected corrective action documentation.	<i>Suggested: Procedures; Non-compliance reports; corrective action plans, corrective action processes, corrective action processes, SSIMS, trending results</i>		
36	Have corrective actions been successful in preventing recurrence (effectiveness)? Are there any “repeat” issues? Reference: PM 12, I 32, 33, 34	Review non-compliance reports and documentation to determine if repeat issues exist.	<i>Suggested: Non-compliance reports; , internal assessment results and external audit results, SSIMS, trend reports</i>		
37	Are corrective actions monitored for timely completion?	Review non-compliance reports and corrective action documentation and interview key S&S staff.	<i>Suggested: Corrective action process and documentation</i>		
38	Are corrective actions verified or validated as closed?	Review non-compliance reports and corrective action documentation and interview key S&S staff.	<i>Suggested: Corrective action documentation, local discrepancy management system</i>		
39	Are effectiveness reviews conducted, in a graded fashion, to determine	Review non-compliance reports and corrective action documentation and	<i>Suggested: Corrective action processes, local discrepancy management system</i>		

PROGRAM REVIEW 10 CFR PART 824 PROGRAM IMPLEMENTATION

#	Question/ Criteria/ Action	Team Action	Documents Reviewed/ Individuals Interviewed	Response/ Comments	Results (S, W/PI, ME, N/A)
	effectiveness of completed actions?	interview key S&S staff.			
40	What do effectiveness reviews reveal? In general, are corrective actions effective? Do you know why/why not?	Review effectiveness review documentation and interview key S&S staff.	<i>Suggested: Corrective action processes, local discrepancy management system</i>		
41	Are most non-compliances self reported?	Review non-compliance records and interview key S&S staff/ management to determine how non-compliances are reported (self or other).	<i>Suggested: Self assessment process, SSIMS, trending results, non-compliance reports</i>		
42	Are there documented processes for self reporting of non-compliances?	Review documents to determine if a standardized self reporting process exists.	<i>Suggested: Program procedures; SSIMS, training course materials, self assessment process</i>		
43	Does a positive self-reporting culture exist?	Interview key line and S&S staff/ management to determine how non-compliances are reported (self or other). Review any other documentation that may support self reporting (e.g., does training and procedures include self reporting).	<i>Suggested: Internal assessment process, local discrepancy management system</i>		
44	Is routine trending and evaluation performed for identified non-compliances (operational data and	Review documentation and interview key S&S staff to determine if a process exists. Review	<i>Suggested: Trend reports</i>		

PROGRAM REVIEW 10 CFR PART 824 PROGRAM IMPLEMENTATION

#	Question/ Criteria/ Action	Team Action	Documents Reviewed/ Individuals Interviewed	Response/ Comments	Results (S, W/PI, ME, N/A)
	issues management)?	records to determine if trending and evaluations have occurred.			
45	Have any trends been identified? Have the trends received the same attention and assignment of actions as the individual non-compliances?	Review documentation and interview key S&S staff	<i>Suggested: Trend reports and associated corrective action plans, internal assessment process</i>		
46	Are complex-wide trends monitored? Are these statistics being used to improve programs?	Review documentation and interview key S&S staff. Also, review Office of Enforcement web site	<i>Suggested: Trending reports</i>		
47	Are lessons learned obtained and/or created and distributed? Reference: A 64	Review documentation and interview key S&S staff	<i>Suggested: Trending results, lesson learned articles</i>		
<b>A</b>	<b>Assessment (Management/Independent), Trending and Continuous Improvement</b>				
48	Do S&S managers assess their management processes?	Review documentation and interview key S&S staff/ managers	<i>Suggested: Internal assessment documentation and process</i>		
49	Is there a documented self assessment plan for the organization/ topical areas?	Review documentation and interview key S&S staff/ managers.	<i>Suggested: Internal assessment documentation and process</i>		
50	Can the manager(s) describe the process used for identifying critical topics for self assessment?	Review documentation and interview key S&S managers.	<i>Suggested: Internal assessment process</i>		
51	Do the assessments include process and	Review documentation and interview key S&S	<i>Suggested: Internal assessment procedures and</i>		

PROGRAM REVIEW 10 CFR PART 824 PROGRAM IMPLEMENTATION

#	Question/ Criteria/ Action	Team Action	Documents Reviewed/ Individuals Interviewed	Response/ Comments	Results (S, W/PI, ME, N/A)
	cultural issues?	staff/ managers.	<i>results</i>		
52	Are assessments performed as planned?	Review documentation and interview key S&S staff/ managers.	<i>Suggested: Internal assessment plans and results</i>		
53	Are assessment results passed on to the appropriate level of management?	Review documentation and interview key S&S staff/ managers, line management.	<i>Suggested: Internal assessment process</i>		
54	Do assessments provide valuable results? Do assessments reflect an appropriate level of depth and breadth? How is assessment data being used to improve operations?	Review documentation and interview key S&S staff/ managers, line management to determine if improvements to operations have been indentified and implemented.	<i>Suggested: Internal assessment process</i>		
55	Are other sources routinely reviewed for deficiencies and/or non-compliances (e.g., daily log reviews, etc.)?	Review program documentation and interview key S&S staff to determine if other sources of information are routinely reviewed.	<i>Suggested: Internal assessment process</i>		
56	Are assessment and other information review results trended? Are results of trending receiving the same attention as deficiencies to include corrective actions and follow-up?	Review program documentation and trending reports.	<i>Suggested: Trend reports; corrective action plans and , local discrepancy management system</i>		
57	Have there been any	Review program	<i>Suggested: Internal</i>		

PROGRAM REVIEW 10 CFR PART 824 PROGRAM IMPLEMENTATION

#	Question/ Criteria/ Action	Team Action	Documents Reviewed/ Individuals Interviewed	Response/ Comments	Results (S, W/PI, ME, N/A)
	“independent” and “external” assessments of the associated topical areas? Are outside parties or peers used to critique security performance – involving the protection of classified information? When?	documentation and interview key S&S staff	<i>assessment and external audit results,, SSIMS</i>		
58	Are results and actions from internal, independent and external assessments being formally identified, entered into a tracking system, addressed and closed in a timely manner?	Review program documentation, systems used, and interview key S&S staff	<i>Suggested: Corrective Action process, SSIM, , local discrepancy management system</i>		
59	Are issues identified through assessments screened or managed in accordance with a grading system (risk based)? Do they also include inadvertent or willful? Do they include extent of condition? Is responsibility assigned?	Review documentation and interview S&S staff to determine if a documented grading system exists. Determine if major non-deficiencies have been identified.	<i>Self Assessment process, Incident reports, local discrepancy management system</i>		
60	Are corrective actions developed for identified deficiencies? Are they based on causal analysis? Does the causal analysis	Review program documentation and interview key S&S staff	<i>Suggested: Corrective action plans, SSIMS, , local discrepancy management system</i>		

PROGRAM REVIEW 10 CFR PART 824 PROGRAM IMPLEMENTATION

#	Question/ Criteria/ Action	Team Action	Documents Reviewed/ Individuals Interviewed	Response/ Comments	Results (S, W/PI, ME, N/A)
	include precursor/ historical reviews?				
61	Are completed actions reviewed for effectiveness? Is there a validation process for completed corrective actions?	Review program documentation and interview key S&S staff	<i>Suggested: Corrective action process and , local discrepancy management system</i>		
62	What other information sources are used to determine issues or potential problem areas?	Interview key S&S staff to determine if other sources of information related to trends, non-compliances, etc. are being used	<i>Suggested: Internal assessment process, external audit results, training results, trending reports</i>		
63	Is continuous improvement demonstrated?	Review program documentation and interview key S&S staff	<i>Suggested: Internal assessment process and trending reports</i>		
64	Are lessons learned shared? Reference: I 47	Review program documentation and interview key S&S staff/ line organization staff	<i>Trending reports and local security bulletins (security awareness)</i>		
<b>R</b>	<b><i>Records and Reporting</i></b>				
65	Are records for non- compliances maintained?	Review sample documentation in the area of incidents, events, assessments, information reviews, tracking and trending to determine if appropriate records are being generated and maintained.	<i>Suggested: Security incident reports; SSIMS, Internal assessment reports; Maintenance reports, local discrepancy management system</i>		
66	Is there a record of the causal analysis method and	Review program documentation and	<i>Suggested: Corrective Action Plans; Critique Reports,</i>		

PROGRAM REVIEW 10 CFR PART 824 PROGRAM IMPLEMENTATION

#	Question/ Criteria/ Action	Team Action	Documents Reviewed/ Individuals Interviewed	Response/ Comments	Results (S, W/PI, ME, N/A)
	results captured in the report/ critique, etc.?	interview key S&S staff	<i>Security incident reports</i>		
67	Are programmatic or repetitive non-compliances captured, documented, and reported?	Review program documentation and interview key S&S staff	<i>Suggested: Trend reports; Internal assessment results</i>		
68	Are there any centralized systems used to capture and track non-compliances?	Review program documentation, systems and interview key S&S staff			
69	Are incidents, assessment and survey results as well as corrective action status reported to DOE as required (i.e., IMI index, SSIMS, etc.) and in accordance with required timeframes?	Review program documentation, systems and interview key S&S staff	<i>Suggested: Security incident reports, SSIMS, local discrepancy management system</i>		

Date(s) Conducted:

Assessors:

Individuals Interviewed: